

REMARKS

Claims 1-75 are currently pending in the subject application and are presently under consideration.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-75 Under 35 U.S.C. §102(e)

Claims 1-75 stand rejected under 35 U.S.C. §102(e) as being anticipated by Bates (US 6,779,021). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Bates, *et al.* does not teach or suggest each and every limitation of appellants' claimed invention.

For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The subject application relates to identification of spam and spam senders at the sender's outgoing message system. For example, the system can perform various counts and compute various scores in order to detect spam senders, as well as, force e-mail senders to perform additional steps or pay fees when they are identified as a potential spam sender. In particular, independent claim 1 (and similarly independent claim 71) recites *a detection component employed by an outgoing message server that detects a potential spammer in connection with at least one outgoing message, the detection of a potential spammer being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account or number of non-deliverable messages sent from the entity's user account.*

Bates, *et al.* does not teach or suggest the aforementioned novel aspects of the subject claims. The cited reference discloses a system that is primarily concerned with detection of spam at recipient's system. The system employs various filters that are based upon counts or keywords in the message in order to determine spam. The cited reference discloses that the filters can be employed at a sender to identify outgoing spam. However, the reference fails to

disclose **an outgoing message server** employing the number of legitimate outgoing messages or the number of non-deliverable messages from a sender in order to determine if the sender is sending spam. The cited reference relies upon generic counts of total outgoing messages or number of recipients in an e-mail message. The Office Action cites Figures 4A and 4B and column 8, line 48-column9, line 2 as teaching *the detection of a potential spammer being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account*. On the contrary this particular section of the cited reference discloses an e-mail server receiving incoming e-mail and determining if the e-mail is spam based upon the number addressees in the e-mail. The number of addressee listed in a received e-mail is not equivalent to the number of apparently legitimate outgoing messages sent from an entity's user account. The reference is silent regarding tracking legitimate outgoing messages from a user account. E-mail being received by an e-mail server cannot be employed to determine number of outgoing messages from a user account. An entity could be sending many outgoing messages that are received by various recipient e-mail servers. Each of these recipient e-mail servers would not necessarily be aware of messages received by the other recipient e-mail serves. Also, for example, spammers often employ other user's account information when sending e-mail that is actually not being sent from the other user's account in order to mislead recipients. Furthermore, the claim clearly states that the detection component is **employed by an outgoing message server**. Bates, *et al.* only discloses an incoming e-mail server analyzing incoming e-mails for spam. Therefore, Bates, *et al.* fails to teach or suggest a detection component employed by an outgoing message server that detects a potential spammer in connection with at least one outgoing message, the detection of a potential spammer being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account or number of non-deliverable messages sent from the entity's user account.

Claim 17 recites *the number of non-deliverable messages is estimated at least in part from failures at message delivery time*. Contrary to assertions in the Office Action, Bates, *et al.* is silent regarding failures at message delivery time. The cited section, column 7, lines 23-47, discusses receipt of messages at an incoming e-mail server where a large number of users are receiving the same or similar messages. At this point the messages have been delivered. Furthermore, the subject claim discloses the outgoing message server performing the detection based upon the number of non-deliverable messages. Bates, *et al.* is only focused on the

incoming e-mail server.

Claim 18 recites *wherein **the number of non-deliverable messages** is estimated at least in part from **Non Delivery Receipts***. Additionally, claims 19-21 recite various limitations related Non Delivery Receipts. The Office Action again cites column 7, lines 23-47 as teaching the limitations of these claims. On the contrary, this section merely discusses a number of users at an e-mail server receiving similar e-mails. Bates, *et al.* is silent regarding the number of non-deliverable messages and non delivery receipts at the outgoing message server.

Independent claim 35 recites *detecting a potential spammer in connection with at least one outgoing message, the detection being based in part on at least one of number of **apparently legitimate outgoing messages sent from an entity's user account** or **number of non-deliverable messages sent from the entity's user account***. As discussed above, Bates, *et al.* fails to teach or suggest an outgoing message server employing the number of legitimate outgoing messages or the number of non-deliverable messages from a sender in order to determine if the sender is sending spam. Figures 4A and 4B and column 8, line 48-column9, line 2 cited in the Office Action relate to recipient counting of received e-mail at an incoming e-mail server. This cannot be employed to determine legitimate outgoing message count, contrary to the assertions in the Office Action. As such, Bates fails to teach all novel features of the subject claim.

Furthermore, claim 38 recites ***computing a total score per sender based upon two or more of the score per outgoing message, the score per sender based at least in part upon outgoing message volume per sender, score per sender based at least in part upon outgoing message rate per sender, the a score per sender based at least in part upon a total recipient count per sender, or the score per sender based at least in part upon a unique recipient count per sender***. Bates, *et al.* discloses various counts but fails to teach combining the counts into a total score for a sender in order to determine if a sender is sending spam. Producing a combined score allows the various sub components of the total score to possibly offset each other or be weighted differently, thereby reducing/increasing the influence of one particular component in determining a spam sender. Bates, *et al.* doesn't teach computing a total score per sender as recited in the subject claim. The Office Action dated November 30, 2007 asserts that the Abstract, column 4, lines 45-51, and column 7, lines 7-12 disclose this feature. On the contrary, the Abstract merely states that e-mails are analyzed and classified as potentially undesirable. Column 4, lines 45-51 and column 7, lines 7-12 states that a percentage of predictability of spam

and a percentage of likelihood as spam respectively is determined for an e-mail message. However, these are not equivalent to computing a total score based upon at least two of *the score per outgoing message, the score per sender based at least in part upon outgoing message volume per sender, score per sender based at least in part upon outgoing message rate per sender, the a score per sender based at least in part upon a total recipient count per sender, or the score per sender based at least in part upon a unique recipient count per sender* as recited in the subject claim. The cited reference fails to discuss how these percentages are computed, and is silent regarding employing two or more of the specific scores recited in the subject claim to compute a total score. In addition, the Office Action dated September 19, 2008 fails to make a specific citation regarding the total score computation of the subject claim. Based upon the above reasoning, Bates, *et al.* fails to teach or suggest all novel features of the subject claim.

Additionally, independent claim 61 (and similarly independent claim 74) recites ***requiring an owner of the user account to resolve one or more challenges after at least one of a number of outgoing messages sent from the user account exceeds a predetermined threshold or a number of recipients counted in one or more sent messages from the user account exceeds a predetermined threshold; and suspending sending of subsequent outgoing messages from the user account until the one or more challenges are resolved.*** Bates, *et al.* is silent regarding requiring the sender of a message to perform any kind of challenge in order to send messages. Additionally, the Office Action fails to cite any specific section of the reference in relation to these limitations of the subject claims.

Moreover, independent claim 65 (and similarly independent claim 75) recites *performing at least one economic analysis to determine **sender outgoing message volume** limits based at least in part on spammer behavior and legitimate user behavior; and ... **limiting the sender outgoing message volume to at least one of a maximum number per challenge resolved or a maximum number per fee paid by a sender.*** The Office Action fails to point to any specific sections of the cited reference that teaches the limitations of these claims. Bates, *et al.* is silent regarding performing any economic analysis, especially one in conjunction with determining sender outgoing message volume limits. The cited reference is also silent regarding user challenges and a message volume fee paid by a sender. As such, Bates, *et al.* fails to teach or suggest the novel features of the subject claims.

Independent claim 72 recites *information employed by an **outgoing message server** associated with detecting spam-like characteristics with at least one outgoing message, the outgoing message comprising at least one of instant message spam, whisper spam, and chat room spam, **the detection being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account or number of non-deliverable messages sent from the entity's user account**, wherein the information determines whether to initiate at least one action that facilitates any one of confirming that the entity is a spammer, mitigating spamming by the entity, or increasing spammer cost.* As noted *supra*, Bates, *et al.* fails to teach an outgoing e-mail server employing the number of legitimate outgoing messages or the number of non-deliverable messages from a sender in order to determine if the sender is sending spam. The cited section relate to recipient counting at an incoming e-mail server, which does not allow for determining the number of apparently legitimate outgoing messages sent from an entity's user account.

Independent claim 73 recites *a means employed by an **outgoing message server** for detecting a potential spammer in connection with at least one outgoing message, the outgoing message comprising at least one of e-mail message spam, instant message spam, whisper spam, and chat room spam, **the detection being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account or number of non-deliverable messages sent from the entity's user account**.* As discussed above, Bates, *et al.* is silent regarding an outgoing e-mail server employing the number of legitimate outgoing messages or the number of non-deliverable messages from a sender in order to determine if the sender is sending spam.

In view of at least the above, it is respectfully submitted that Bates, *et al.* does not teach or suggest applicants' invention as recited in independent claims 1, 35, 61, 65, and 71-75 (and claims 2-34, 36-60, 62-64, and 66-70 which respectively depend there from) and thus fails to anticipate the subject claims. Accordingly, withdrawal of this rejection is respectfully requested.

II. Rejection of Claims 61-70 and 74 Under 35 U.S.C. §102(e)

Claims 61-70 and 74 stand rejected under 35 U.S.C. §102(e) as being anticipated by Wilson (US 2004/0015554). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Wilson does not teach or suggest each and every limitation of

appellants' claimed invention.

Independent claim 61 (and similarly independent claim 74) recites ***requiring an owner of the user account to resolve one or more challenges after at least one of a number of outgoing messages sent from the user account exceeds a predetermined threshold or a number of recipients counted in one or more sent messages from the user account exceeds a predetermined threshold; and suspending sending of subsequent outgoing messages from the user account until the one or more challenges are resolved.***

Contrary to assertions in the Office Action, Wilson does not teach or suggest the aforementioned novel aspects of the subject claims. Cited figures 1, 2, 3, 5, Abstract, and paragraphs 61-63 of Wilson disclose identification of spam at a recipient's incoming mail system. The system employs an address filter to let through accepted addresses and send blocked addresses to a rejected folder. Unknown addresses cause a challenge to be sent to the sender to help validate the sender as legitimate or a spam sender. Senders who respond to the challenge correctly, are added to a list of allowed senders, and those that do not respond appropriately are added to a list of blocked senders. The cited reference relies on identifying spam at the recipient's incoming mail system, **where as the subject claims detect spam senders based upon the senders outgoing mail and take actions to suspend the senders account** when appropriate. The subject claim employs techniques to identify senders of spam at the sender's outgoing e-mail system and then based upon thresholds of outgoing message indicative of spam, will stop sending of outgoing messages until the sender has completed a challenge. In the system of Wilson, a sender is not restricted from sending messages in any way. Likewise, the cited reference is silent regarding monitoring various features of outgoing messages for a sending entity to identify spam: outgoing message volume monitoring, total outgoing message recipient counting, outgoing message unique recipient counting, outgoing message rate monitoring, number of apparently legitimate outgoing messages, or number of non-deliverable messages for an entity. Wilson is focused on the incoming e-mail server which does not have the ability to suspend outgoing messages from a user account of a sending address listed in an incoming e-mail.

In view of at least the above, it is respectfully submitted that Wilson does not teach or suggest applicants' invention as recited in independent claims 61 and 74 (and claims 62-64

which respectively depend there from) and thus fails to anticipate the subject claims. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP418US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Nilesh S. Amin/

Nilesh S. Amin

Reg. No. 58,407

AMIN, TUROCY & CALVIN, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731